User Guide
Managed VPN Router

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing.
Wireless Maingate AB shall have no liability for any error or damages of any kind resulting from use of this document.

Revision: 1.0

maingate

ADDRESS: BOX 244, SE-371 24 KARLSKRONA, SWEDEN
VISITORS: DROTTNINGGATAN 16
PHONE. +46 455 36 37 00 FAX: +46 456 36 37 37
WEB: WWW.MAINGATE.SE

Table of Contents

1	Introduction	3
2	Service overview	3
2.1	Customer Requirements	3
3	Set up of Managed VPN router	4
4	IP Configuration	7
4.1	Maingate VPN tunnels	7
4.2	IP Routing	7
4.3	Firewall Configuration	8
4.3.1	Firewall between MVR routers and Internet	8
4.3.2	Firewall on Access network	9
5	Installation	10
5.1	Attaching routers to network	10
6	Appendix	11
6.1	Terminology	11

1 Introduction

This document is intended to be used by the customer whenever ordering, configuring or using the Maingate Managed VPN Router product.

2 Service overview

Maingate Managed VPN Router service provides secure IP communication between the customer's network and Maingate's networks and services. This service can be used for any of Maingate's IP based services. An overview of the functionality is shown in figure 1 below.

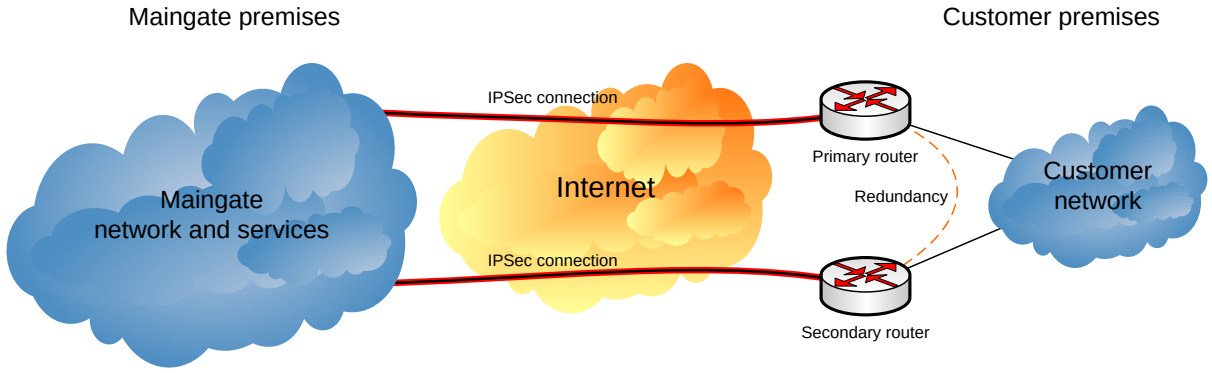


Figure 1 – Service overview

The customer application is connected to Maingate over the Internet using VPN tunnels. Each router has a redundant *IPSec* tunnel connected to a core router. To avoid IP addressing conflicts, the access network is a public IP-address network, provided by Maingate.

2.1 Customer Requirements

In order for the MVR service to function as expected, the customer's network must meet the following requirements:

- Network must be set up to allow both routers to communicate on Access network.
- Access to the Internet with two public IP-addresses that should be assigned to MVR routers. These addresses do not need to be on the same public network.
- If MVR routers are installed behind a firewall, traffic described in 4.3.1 must be allowed to pass through.

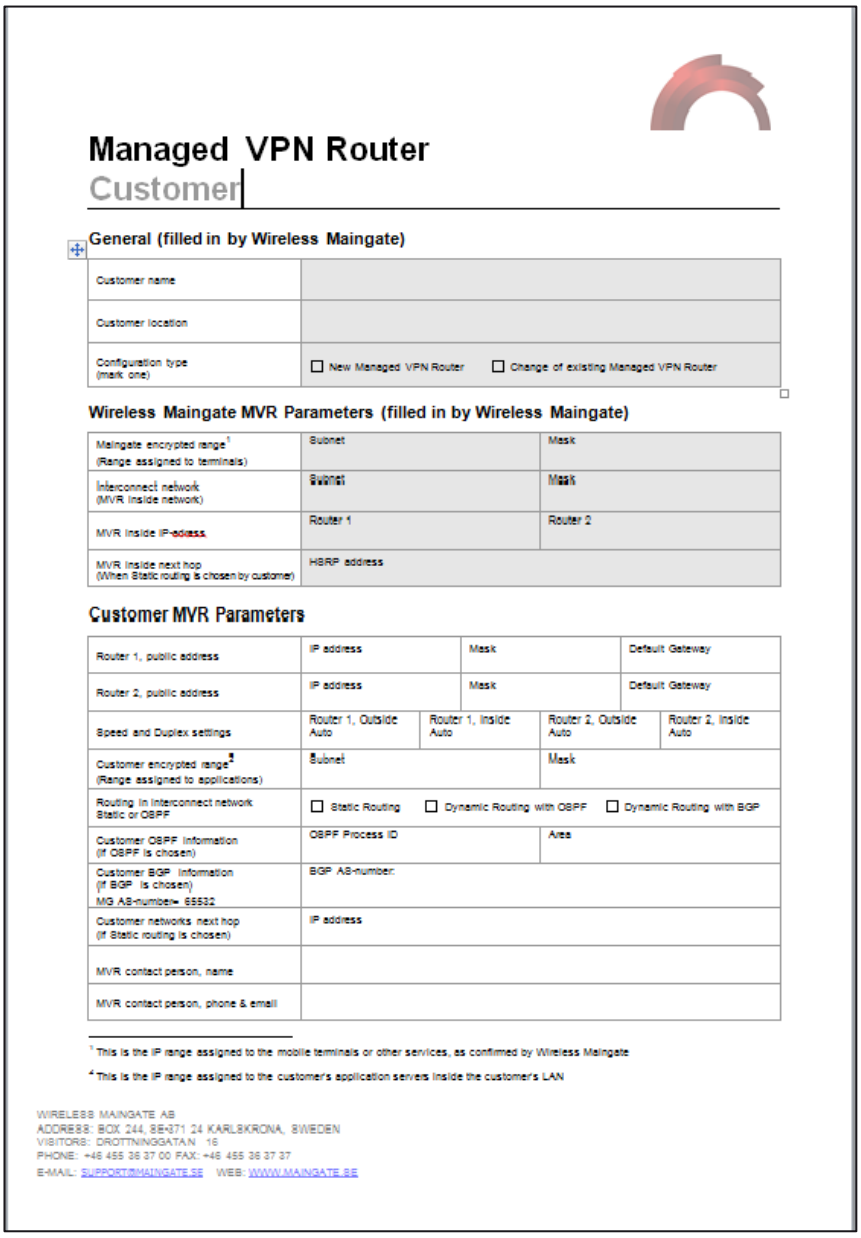
3 Set up of Managed VPN router

Once the customer has ordered the Managed VPN router service, Maingate will configure the new account. Subsequently a confirmation mail with be sent to the Main Contact Person and the Technical Contact Persons. Two documents will be attached to the confirmation e-mail:

Managed VPN Router User Guide (this document)

Managed VPN Router Configuration Form

The Configuration Form must be completed by the customer in order for Maingate to configure the routers.



Managed VPN Router

Customer

General (filled in by Wireless Maingate)

Customer name	
Customer location	
Configuration type (mark one)	☐ New Managed VPN Router ☐ Change of existing Managed VPN Router

Wireless Maingate MVR Parameters (filled in by Wireless Maingate)

Maingate encrypted range[1] (Range assigned to terminals)	Subnet	Mask
Interconnect network (MVR inside network)	Subnet	Mask
MVR inside IP-address	Router 1	Router 2
MVR inside next hop (When Static routing is chosen by customer)	HSRP address	

Customer MVR Parameters

Router 1, public address	IP address		Mask	Default Gateway
Router 2, public address	IP address		Mask	Default Gateway
Speed and Duplex settings	Router 1, Outside Auto	Router 1, Inside Auto	Router 2, Outside Auto	Router 2, Inside Auto
Customer encrypted range[2] (Range assigned to applications)	Subnet		Mask	
Routing in Interconnect network Static or OSPF	☐ Static Routing	☐ Dynamic Routing with OSPF	☐ Dynamic Routing with BGP	
Customer OSPF information (if OSPF is chosen)	OSPF Process ID		Area	
Customer BGP information (if BGP is chosen) MG AS-number= 65532	BGP AS-number:			
Customer networks next hop (if Static routing is chosen)	IP address			
MVR contact person, name				
MVR contact person, phone & email				

[1] This is the IP range assigned to the mobile terminals or other services, as confirmed by Wireless Maingate

[2] This is the IP range assigned to the customer's application servers inside the customer's LAN

WIRELESS MAINGATE AB
ADDRESS: BOX 244, SE-371 24 KARLSKRONA, SWEDEN
VISITORS: DROTTNINGGATAN 16
PHONE: +46 455 36 37 00 FAX: +46 455 36 37 37
E-MAIL: SUPPORT@MAINGATE.SE WEB: WWW.MAINGATE.SE

Figur 2 – MVR configuration form

Router 1 and 2, public IP address	Two public IP addresses accessible over the Internet will be assigned to MVR routers outside interface.
Speed and Duplex settings	Speed and duplex settings for MVR router interfaces to match customer equipment. Enter values in format “speed/duplex”, ex “auto”, “100/full” or “10/half”.
Customer encrypted range	The network(s) from which customer will access Maingate services.
Routing in access network	Routing mechanism used between MVR routers and customer equipment. Possible values are“Static” , “OSPF” or “BGP”.
Customer OSPF information	OSPF Process and Area identifier. Only entered if OSPF routing is chosen.
Customer networks next hop	Gateway for MVR routers on the inside interfaces. Customer encrypted range will be routed to this point. Only entered if static routing is chosen.

4 IP Configuration

In order for MVR to function correctly, the transmission of IP packets between Maingate and the customer must be carefully configured. This chapter describes how the customer should set up and configure their systems and networks to be compatible with the MVR solution.

4.1 Maingate VPN tunnels

IPSec encryption is used for the VPN tunnel between Maingate and the LAN connecting the customer network. IPSec is a set of standard protocols for implementing secure communication and encryption key exchange between computers.

An IPSec VPN generally consists of two communication channels between the endpoint hosts: a key-exchange channel over which authentication and encryption key information is passed, and one or more data channels over which private network traffic is carried.

4.2 IP Routing

Once the MVR routers have been set up, the customer's LAN must be configured to route applicable packets through them and allow packets from Maingate network to reach the customer application via MVR routers. There are two ways of configuring this; static routing with HSRP redundancy or OSPF/BGP with routing redundancy. The figure below shows an example of how static routing could be set up. Please note that Maingate does *not* require customer to have redundant connections or firewalls as shown below.

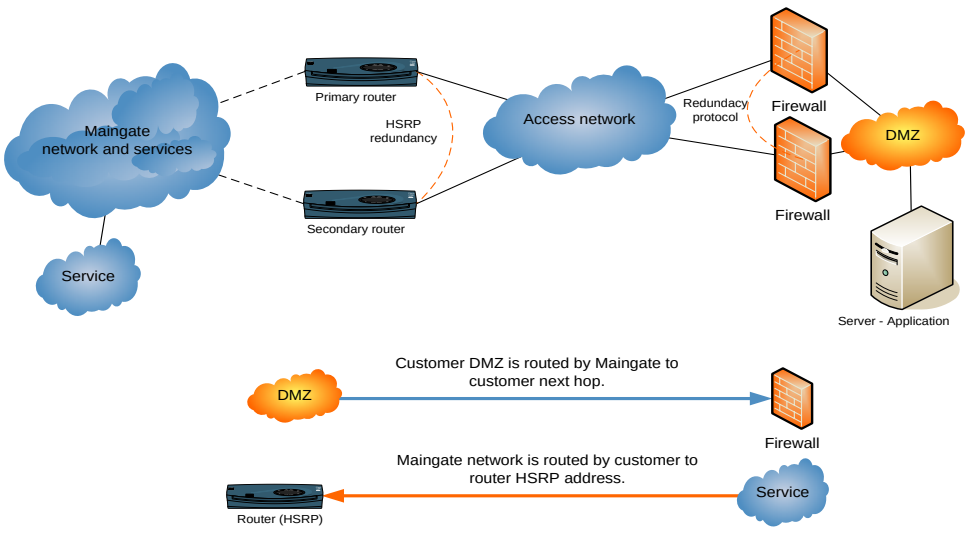


Figure 3 –IP routing between Maingate and customer with HSRP

On both MVR routers and customer firewalls or equivalent equipment, a virtual interface is configured. These virtual interfaces are used for routing to handle redundancy. If a router or tunnel breaks down, the virtual interface will move to the standby router. Hence, there will only be traffic on one tunnel at a time.

An example of OSPF configuration is shown below.

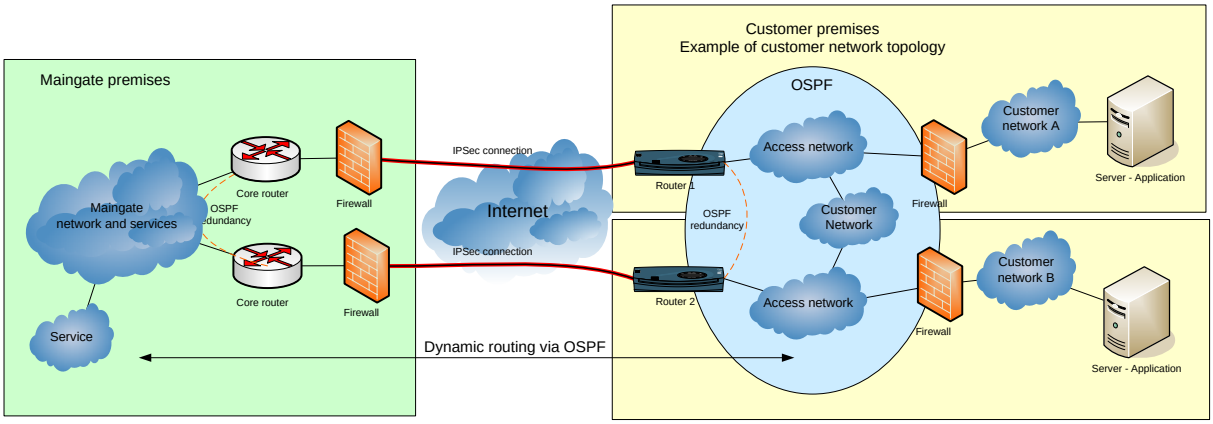


Figure 4 –IP routing between Maingate and customer with OSPF

The inside networks on the Managed VPN routers share routing information with the customer network using a dynamic routing protocol such as OSPF. Routing of the customer networks will then be redirected to Maingate's network via both routers and vice versa. There is no hard-configured primary or secondary router, as OSPF will choose the best path between Maingate and the customer networks. If a router malfunctions or a tunnel breaks down, the routing protocol will update the paths and send all traffic through one tunnel.

The actual IP-addresses to use and networks to be routed are specified on the MVR configuration form.

4.3 Firewall Configuration

Maingate does not require any firewalls for the MVR service. However, when using IP-based communication, special attention must be paid to providing adequate security for the systems and information. Since using some of Maingate's services effectively expands the customer's LAN to a multitude of connection points, special attention to security is appropriate.

4.3.1 Firewall between MVR routers and Internet

The customer must ensure that the customer's firewall is open to permit the types of IP sessions that Wireless Maingate uses for VPN connection and remote access.
The following traffic must be allowed to pass through the firewalls to MVR routers:

- SSH from 87.237.152.140 and 83.241.178.2
- ESP bi-directional with 87.237.152.33
- ESP bi-directional with 83.241.178.2
- IKE (udp 500) bi-directional with 87.237.152.33
- IKE (udp 500) bi-directional with 83.241.178.2

4.3.2 Firewall on Access network

The customer must ensure that the customer's firewall is open to allow the types of IP sessions that are used by terminal and application. If not, the IP packets will be blocked and communication will not function correctly. Maingate's firewall towards the VPN tunnel is open to allow for all types of IP sessions.

5 Installation

5.1 Attaching routers to network

Maingate will deliver two preconfigured routers which should be installed by the customer. Both routers should be connected as shown in figure 6 below.

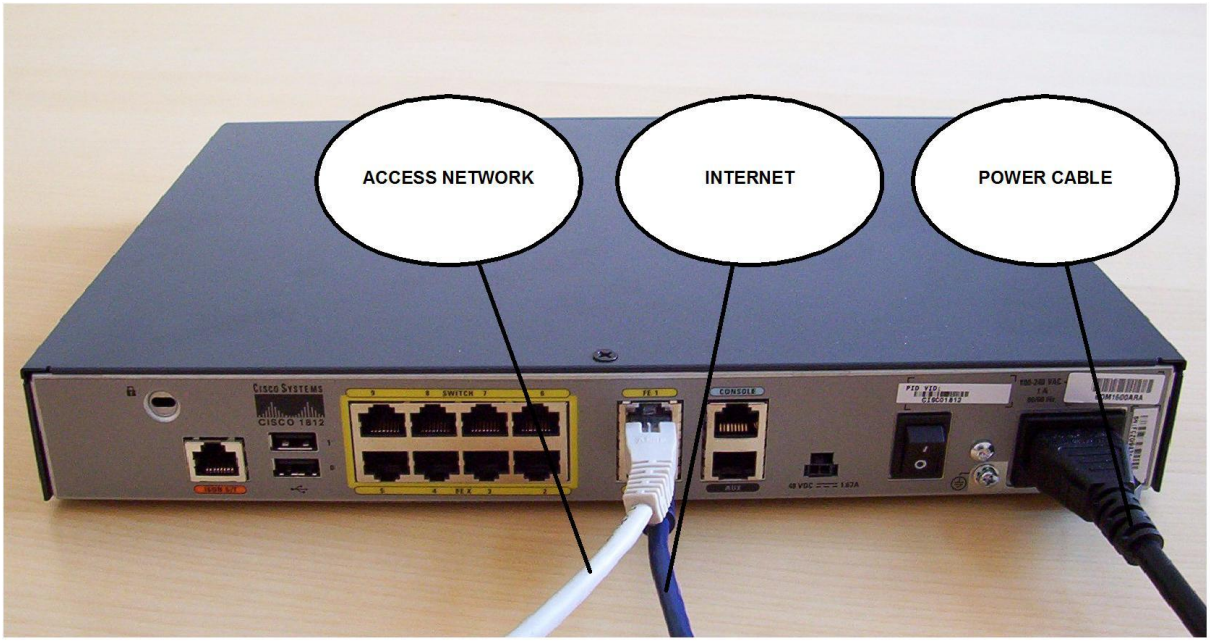


Figure 5 – How to connect MVR routers

The customer should connect Internet to the lower outlet marked as “FE0” and the access network to the upper outlet marked as “FE1”.

Maingate recommends that the routers are placed physically apart and with redundant power supply.

Note: The routers are not delivered to the customer until the MVR configuration form has been correctly filled in.

6 Appendix

6.1 Terminology

Access Network	The network that connects the MVR routers with customer's routing equipment. Also called interconnect network.
HSRP	Hot Standby Router Protocol
IP Default Route	Default destination of unrouted IP packets
IPSec	Internet Protocol Security
LAN	Local Area Network
MVR	Managed VPN Router
OSPF	Open Shortest Path First (Routing protocol)
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network